4.1.5 Security and Accountability Activities

Security Management

Security management addresses the following:

- Establishment of policy and procedures for security
- Management of the authentication and authorization databases
- Intrusion prevention/detection
- Security event logging and resolution
- Report generation

Security Management provides for the management of the security mechanisms that are used to protect and control access to ECS data, control and processing resources. It provides the rules and the implementation for the following:

- authentication procedures
- maintenance of authorization facilities
- maintenance of security logs
- intrusion detection
- recovery procedures

The mechanisms used to provide security in ECS comprise three distinct parts:

- network security
- distributed communications security
- host-based security.

Network security management involves the management of routing tables used for address-based filtering (network authorization). This is implemented through router COTS configuration files through which access control rules are specified.

The management of distributed communications security involves the management of the authentication database (the DCE registry database), the authorization database (DCE Access Control List Managers). This is implemented through the use of DCE Cell Manager. The DCE Cell Manager is a COTS product that provides a Motif-based capability to administer the DCE security registry (authentication database), and the access controls on cell resources (authorization database).

Host-based security management provides the control of access to and the protection of these mechanisms, in addition to the management of compliance to established security policy (e.g. password usage guidelines), and intrusion detection (e.g. break-ins). Access control to network services is provided by TCP wrappers, a public domain tool. Compliance management is provided through the public domain products npasswd, crack, and SATAN. Intrusion detection and alerts are provided by the public domain product Tripwire, and custom development.

Site Security Management:

1. Manages security of local databases.
2. Manages compliance to security directives and guidelines established and disseminated by the SMC.
3. Performs intrusion detection checks in order to maintain the integrity of ECS resources.
4. Provides automatic alerts for intrusion events.
5. Provides the capability to analyze security audit trails.
6. Provides the mechanisms to generate reports of security activities.
7. Implements contingency Plans.

SMC Security Management Application Service is responsible for establishing and disseminating security guidelines to the sites, disseminating security advisories received from external systems (security agencies such as CERT) to the sites, receive security reports from the sites, and to receive notifications of and coordinate the recovery from detected security breaches at the sites and external systems.

Accountability Management

The Accountability Management provide User Registration and the generation of reports from audit trails.

ECS provides for two generic classes of users: guest users and registered users. Guest users are users that have not formally registered as registered users. Registered users are those guest users that have submitted requests for a registered user account, and have had accounts created for them, based on an approval process. Registered users are allowed access to services and products beyond those available to guest users.

Guest users are provided the capability to submit a request for a registered user account, which is captured into a database of pending requests. Operators may access this database of pending requests in the process of user registration, in order to create a registered user account from a list of pending requests.

User registration provides the operators the capability to create accounts against requests submitted by guest users wishing to become authorized ECS users. The registration service provides the capabilities for the creation, modification and maintenance of accounts with user profiles.

The user profile contains information about the user. This includes the name of the user, access privileges, a user identification code, the user's primary DAAC, the organizational affiliation, investigating group (such as an instrument team) affiliation (if any), the project the user is affiliated with, the name of the PI of the project, the mailing address of the user, the shipping address to which data needs to be sent, media preferences for orders, the user's telephone number and the user's electronic mail address (if any).

The Audit Trail capability provides the means to verify the integrity of the system. This comprises the generation of a user audit trail and a security audit trail.

4.1.5.1 Security Management Scenario

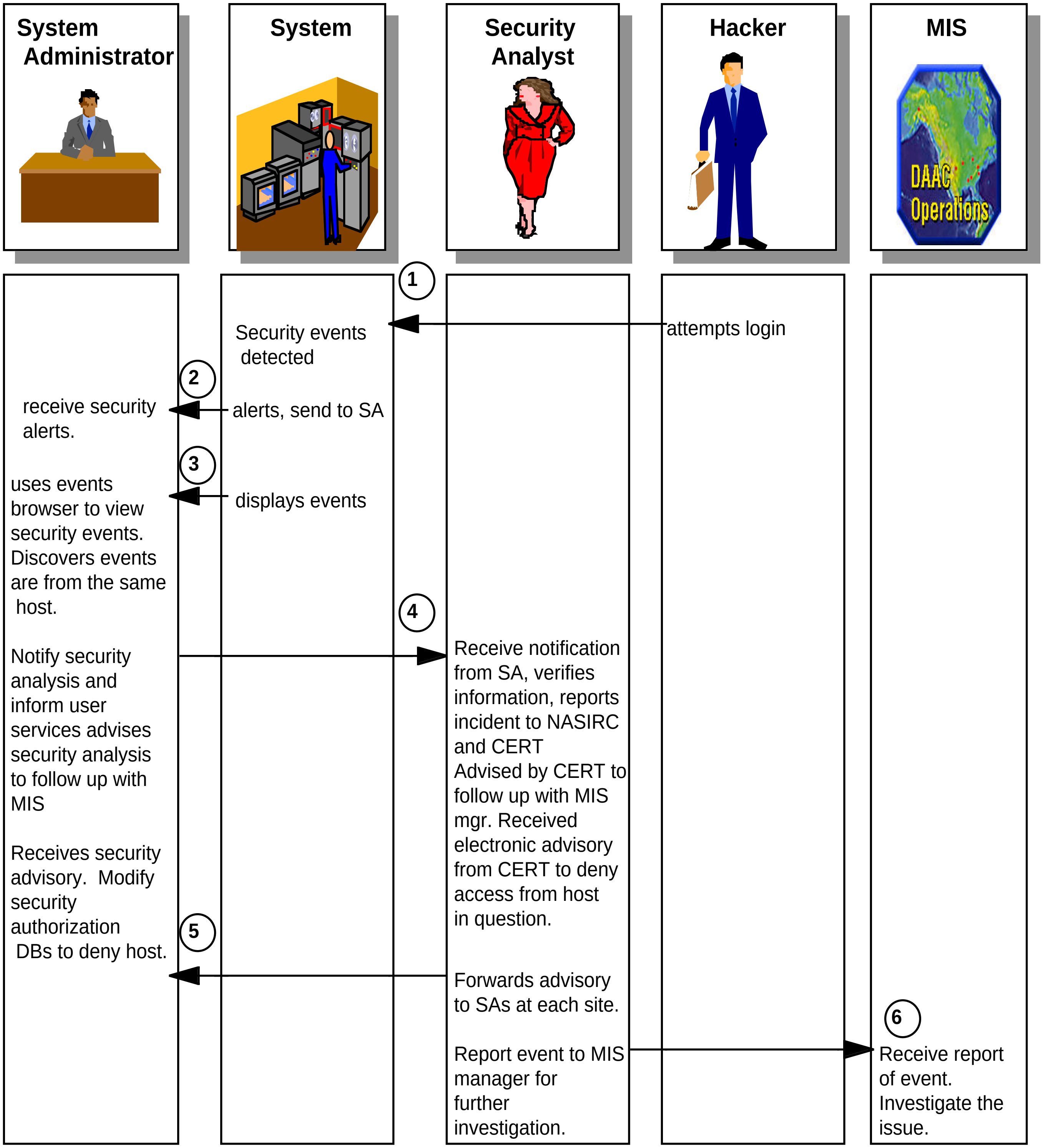
This scenario, depicted in Figure 4.1.5.1-1 and Table 4.1.5.1-1, describes a breakin attempt by a "hacker" from an SCF, and illustrates information flows associated with the reporting of security incidents by a DAAC to the SMC. It further describes how the SMC forwards (reports) the incident to external security agencies such as the CERT and the NASIRC for the purpose of coordination of recovery action; and how security advisories and security directives received from agencies such as the CERT are flowed down to the DAACs. Table 4.1.5.1-1 identifies the system-operator actions with data exchanged and a scenario text description.

Assumption: The Security Management Application has been set up to send an alert to the Systems Administrator (SA) upon the occurrence of five login failures from any given source. The subnetwork of a user at an SCF is allowed access to ECS.

A “hacker” at the SCF campus (who discovers the hosts at the DAAC) attempts to log into ECS by guessing passwords. The hacker tries a new host after five login failures at a given host. The Security Management Application detects the security events when the established thresholds have been crossed. As a result, the SA receives multiple security alerts. The SA, during investigation, retrieves security events in the events browser window. The SA discovers that the login attempts on the multiple hosts originated from the same host, which is in the same domain as the SCF.

The SA calls the Security Analyst at the SMC and User Services to apprise them of the information. The Security Analyst at the SMC, after verifying the information, calls NASIRC and CERT to report the incident. He is advised to follow up with the MIS manager at the SCF campus; and is sent an electronic advisory to direct all ECS sites to explicitly deny all incoming accesses from the host in question.

The Security Analyst at the SMC forwards the security advisory to User Services and the SAs at all sites. Based on this advisory, the SAs at all the sites modify the network security authorization databases to deny all incoming accesses from the host in question. The Security Analyst reports the event to the MIS manager at the SCF campus who proceeds to have the issue investigated.



attempts login

Security events detected

alerts, send to SA

receive security alerts.

displays events

uses events browser to view security events. Discovers events are from the same host.

Notify security analysis and inform user services advises security analysis to follow up with MIS

Receive notification from SA, verifies information, reports incident to NASIRC and CERT Advised by CERT to follow up with MIS mgr. Received electronic advisory from CERT to deny access from host in question.

Receives security advisory. Modify security authorization DBs to deny host.

Forwards advisory to SAs at each site.

Report event to MIS manager for further investigation.

Receive report of event. Investigate the issue.

Figure 4.1.5.1-1. Security Management

Table 4.1.5.1-1. Security Management

Step	Operator/User	System	Purpose
1	A "hacker" at the SCF campus (who discovers the hosts at the DAAC) attempts to log in by guessing passwords. The "hacker" tries a new host after five login failures at a given host.	The Security Management Application (SMA) detects the security events when the established thresholds have been exceeded.	SMA detects security events.
2	The Systems Administrator (SA) receives multiple security alerts.	The SMA sends alert of security event to the SA.	Notification of security event.
3	The SA , during investigation, retrieves security events in the browser window. The SA discovers that the login attempts on the multiple hosts originated from the same host, which is in the same domain as the SCF.	Security events are displayed in the events browser window.	View security events, determine domain of originating host.
4	The SA calls the Security Analyst at the SMC to apprise him of the event information, and informs User Services. The Security Analyst at the SMC, after verifying the information, calls NASIRC and CERT to report the incident. The Security Analyst at the SMC is advised to follow up with the MIS manager at the SCF campus; and receives an electronic advisory from CERT to direct all ECS sites to explicitly deny all incoming accesses from the host in question.		Notification to CERT, NASIRC, and User Services of the security event. CERT sends directive to Security Analyst.
5	The Security Analyst at the SMC forwards the security advisory from CERT to User services and the SAs at all sites. Based on this advisory, the SAs at all the sites modify the network security authorization databases to deny all incoming accesses from the host in question.		Sites are directed to deny access to the host in question.
6	The Security Analyst reports the event to the MIS Manager at the SCF campus who proceeds to have the issue investigated.		Notify MIS manager for further investigation.

4.1.5.2 Accountability Management Scenario

This scenario, depicted in Figure 4.1.5.2-1 and Table 4.1.5.2-1, describes how an approved request for a registered user account (approved via an established approval process) is created, and how the password and instructions on the use of the account are sent to the user.

The Systems Administrator (SA) invokes the user registration sequence, and selects the option to add a new user to the system. The system displays, in tabular form, a list of all the pending requests for registered user accounts, from which the SA selects the entry corresponding to the approved account. The details filled in by the user are displayed, in response to which the SA fills in additional fields, creates the account and assigns a password. Finally the SA prints the account/password details, along with instructions on how to access the account to the newly registered user.

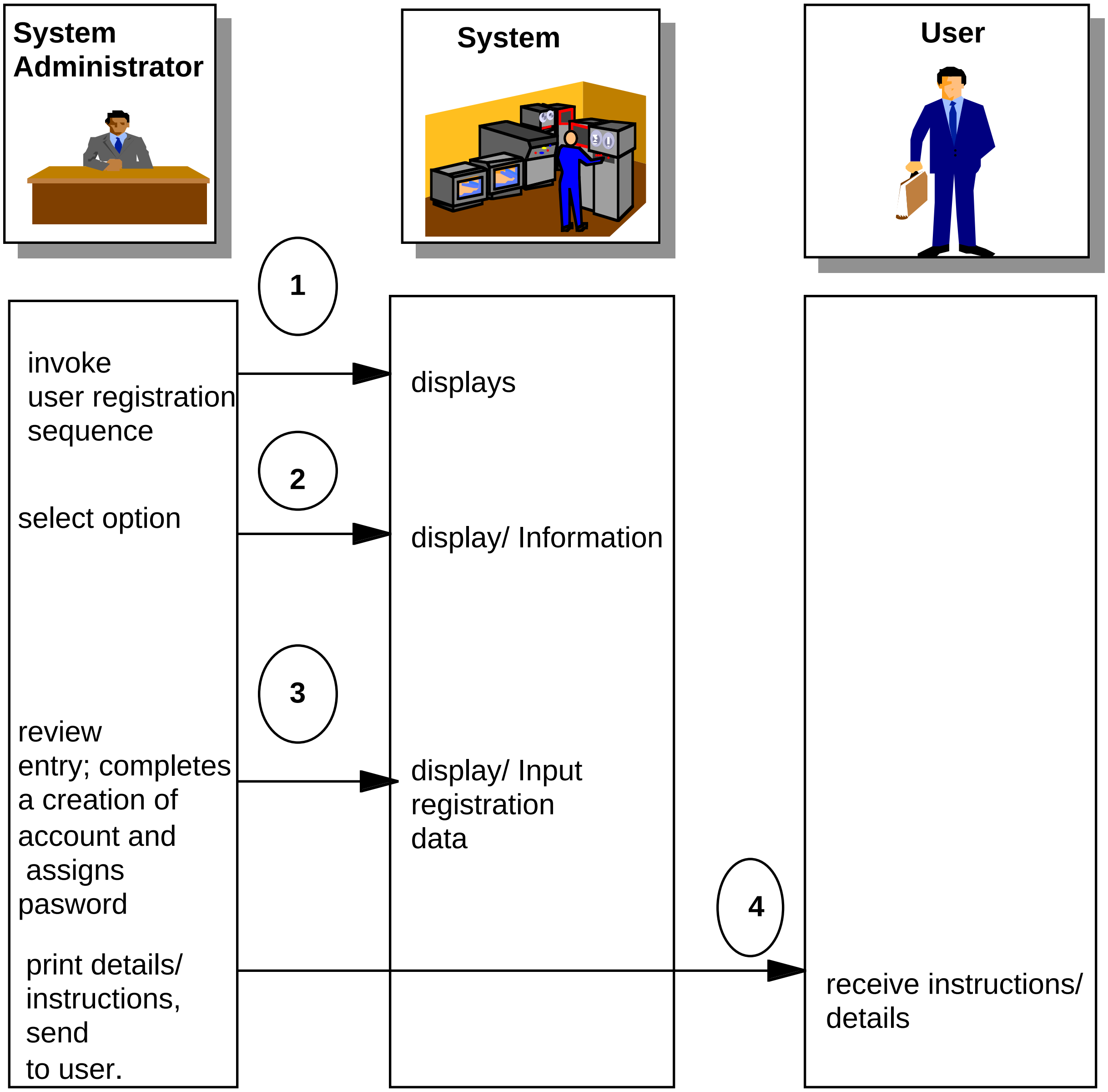

System Administrator
System
User
1
2
3
4
invoke user registration sequence
select option
review entry; completes a creation of account and assigns pasword
print details/ instructions, send to user.
displays
display/ Information
display/ Input registration data
receive instructions/ details

Figure 4.1.5.2-1. Accountability Management

Table 4.1.5.2-1. Accountability Management

Step	Operator/User	System	Purpose
1	The Systems Administrator (SA) invokes the user registration sequence.	Displays a list of all pending requests for registered user accounts	Display list of pending user accounts.
2	The SA selects the option to add a new user to the system and selects the entry corresponding to the approved account.	Display/Input user registration options.	Select user account for registration.
3	The SA reviews the entry corresponding to the approved account. The SA views the details filled in by the user, and in response, fills in additional fields, creates the account, and assigns a password.	Displays data provided by the user, and enables the SA to fills in additional fields.	Create account.
4	The SA prints out the account/password details, along with instructions on how to access the account by the newly registered user, and sends to the user.		Print out account details/instructionand send to user.

4.1.6 Resource Planning (Scheduling) Activities

Resource planning has two facets - local or DAAC resource planning as well as system planning. These activities include the scheduling of site/system resources for ground events such as:

- preventative maintenance
- testing
- simulations

The Planning Subsystem provides tools to allow DAAC-wide resource planning. These tools allow a resource planner to schedule activities that require the use of a system resource. The Planning Subsystem will then take into account these resource ground events when planning production.

The planning of ground events on resources within a DAAC are carried out by the site resource planner using the Planning Workbench utility within the Planning Subsystem. This utility allows the planner to specify predictable ground events against ECS resources.

At PDPS database initialization, the MSS Resource Configuration Information is used to identify the current resources available. Resources are defined for the whole DAAC and include computers, disks, and networks. The Planning Workbench builds resource models from these defined resources. This configuration information can then be updated by MSS whenever there is a change.

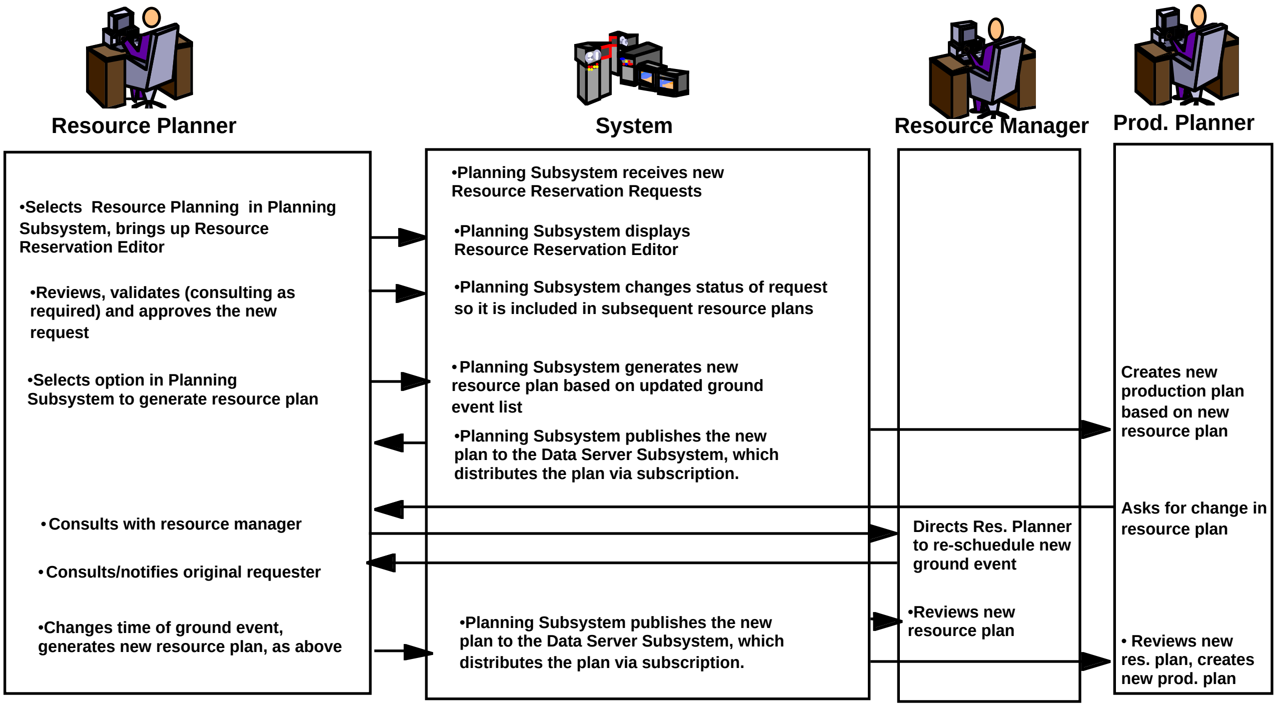
Once these resources are identified, the resource planner at each site can identify ground events that need to be scheduled. These events may consist of testing, simulations, preventative maintenance or upgrades, or any other event that takes resource.   These events are entered with an activity description, resource requirements, time requested (both preferred and acceptable variances), and a duration into the PDPS database using a Planning Workbench editor .

Resource planning can take place whenever a production plan needs to be created. In general, this will occur on a biweekly basis for 30 day plans, on a weekly basis for 10 day plans, and on a daily basis. Ground events can be entered at any time however, and a replan may be done whenever it is necessary. In addition, the extent of the plan is a configurable item so DAAC personnel can choose the period that best meets their needs.

Schedule adjudication is supported by the System Management Center (SMC) and will be assisted by tools provided by the Planning Subsystem. Plans, provided by each DAAC, can be displayed at the DAACs and the SMC so that conflicts can be identified. Coordination between the DAACs involved and the SMC becomes an iterative process of replanning until the conflicts are resolved. Once candidate plans that meet all schedules are produced, these plans can be activated.

4.1.6.1 Planning Production Resources Scenario

The following scenario, depicted in Figure 4.1.6.1-1 and Table 4.1.6.1-1, is assumed to occur during a given day of the Release B period at the LaRC DAAC. The system at the DAAC is in stable operations. The scenario describes the process for entry of ground events into the resource planning system by the resource planner. A resource request for a hardware maintenance activity against a production processor due in 3 weeks is forwarded to the resource planner. This request is entered into the system by the Resource Planner, who requests that the Production Planner generate a new candidate plan with this new resource reservation in it to ensure that production is not overly impacted. The Production Planner notices that this ground event does impact the completion time of a production request, and asks that it be reschedule for later in the week. The Resource Manager directs the Resource Planner to reschedule the event and a new Resource Plan is generated.



•Selects Resource Planning in Planning Subsystem, brings up Resource Reservation Editor

•Reviews, validates (consulting as required) and approves the new request

•Selects option in Planning Subsystem to generate resource plan

• Consults with resource manager

• Consults/notifies original requester

•Changes time of ground event, generates new resource plan, as above

•Planning Subsystem receives new Resource Reservation Requests

•Planning Subsystem displays Resource Reservation Editor

•Planning Subsystem changes status of request so it is included in subsequent resource plans

• Planning Subsystem generates new resource plan based on updated ground event list

•Planning Subsystem publishes the new plan to the Data Server Subsystem, which distributes the plan via subscription.

•Planning Subsystem publishes the new plan to the Data Server Subsystem, which distributes the plan via subscription.

Directs Res. Planner to re-schuedule new ground event

•Reviews new resource plan

Creates new production plan based on new resource plan

Asks for change in resource plan

• Reviews new res. plan, creates new prod. plan

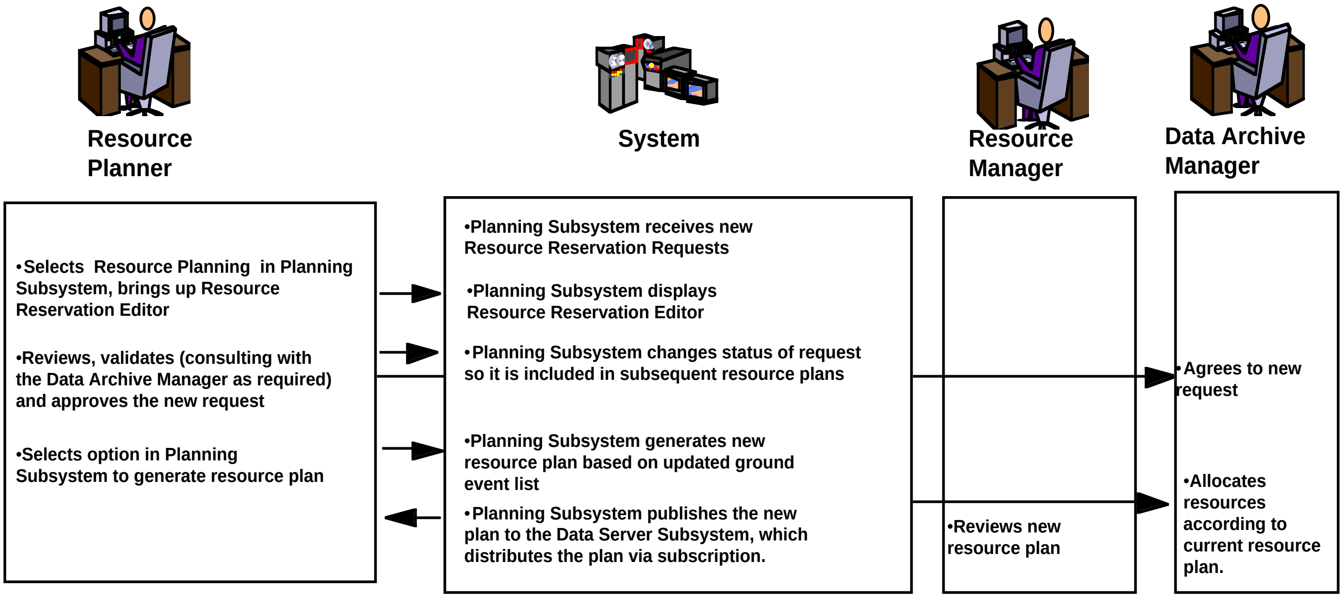
Figure 4.1.6.1-1   Planning Production Resources Scenario

Table 4.1.6.1-1. Planning Production Resources Scenario

Step	Operator/User	System	Purpose
1	DAAC Resource Planner receives request for a resource reservation for some of the production resources for preventative maintenance		Receive Resource Reservation Request
2	DAAC Resource Planner uses the Resource Request Editor to enter the request into the system, validates it and approves it.	Resource Planning accepts the resource reservation request, marks it as validated, and compares it with other resource reservation to ensure that there is no conflict	Enter Resource Reservation Request
3	DAAC Resource Planner selects option to generate a new Resource Plan and publishes it	Resource Planning displays a timeline of the resource reservations currently approved in the system.	Display Resource Plan
4	DAAC Production Planner generates a new candidate plan based on the current resource plan.	Production Planning Workbench generates a new candidate plan with the new resource reservation in it.	Create Production Plan
5	DAAC Resource Planner uses the Resource Request Editor to modify the times of the request and approves it.	Resource Planning accepts the updated resource reservation request and compares it with other resource reservation to ensure that there is no conflict	Update Resource Reservation Request
6	DAAC Resource Planner selects option to generate a new Resource Plan and publishes it	Resource Planning displays a timeline of the resource reservations currently approved in the system.	Display Resource Plan

4.1.6.2 Planning Ingest Resources Scenario

The following scenario, depicted in Figure 4.1.6.2-1 and Table 4.1.6.2-1, is assumed to occur during a given day of the Release B period at the Goddard DAAC. The system at the DAAC is in stable operations. The scenario describes the process for entry of ground events into the resource planning system by the resource planner. A resource request for a training activity against an ingest processor due next week is forwarded to the resource planner. This request is entered into the system by the Resource Planner, who confers with the Data Archive Manager and decides to approve the event, and a new resource plan is generated and published to the Data Server. The Data Archive Manager receives a copy of the Resource Plan via subscription and allocates the resource reservation resources according to the resource plan.



Resource Planner

- Selects Resource Planning in Planning Subsystem, brings up Resource Reservation Editor
- Reviews, validates (consulting with the Data Archive Manager as required) and approves the new request
- Selects option in Planning Subsystem to generate resource plan

System

- Planning Subsystem receives new Resource Reservation Requests
- Planning Subsystem displays Resource Reservation Editor
- Planning Subsystem changes status of request so it is included in subsequent resource plans
- Planning Subsystem generates new resource plan based on updated ground event list
- Planning Subsystem publishes the new plan to the Data Server Subsystem, which distributes the plan via subscription.

Resource Manager

- Reviews new resource plan

Data Archive Manager

- Agrees to new request
- Allocates resources according to current resource plan.

Figure 4.1.6.2-1. Planning Ingest Resources Scenario

Table 4.1.6.2-1. Planning Ingest Resources Scenario

Step	Operator/User	System	Purpose
1	DAAC Resource Planner receives request for a resource reservation for some of the production resources for preventative maintenance		Receive Resource Reservation Request
2	DAAC Resource Planner uses the Resource Request Editor to enter the request into the system, validates it and approves it.	Resource Planning accepts the resource reservation request, marks it as validated, and compares it with other resource reservation to ensure that there is no conflict	Enter Resource Reservation Request
3	DAAC Resource Planner selects option to generate a new Resource Plan and publishes it	Resource Planning displays a timeline of the resource reservations currently approved in the system.	Display Resource Plan
4	DAAC Data Archive Manager allocates the resource according to the new resource plan		Allocate Resources

4.1.6.3 Schedule Adjudication Scenario

See Figure 4.1.6.3-1 for a pictorial representation and Table 4.1.6.3-1 for a sequence of events for the Schedule Adjudication Scenario.

This scenario involves coordinating production schedules between two DAACs. The Production Scheduler at DAAC "A", upon updating the DAAC's 30-day production plan, discovers that a high priority job scheduled 7 days from now will have to be delayed a day due to a change in the Data Availability Schedule (DAS) from DAAC "B".

The Production Scheduler at DAAC "A" displays the revised 30-day plan and determines that the job priority warrants that the delay should be eliminated or reduced. The scenario assumes that attempts to resolve the conflict directly between DAAC "A" and DAAC "B" were unsuccessful and, therefor, it must be adjudicated by the SMC. The Production Scheduler at DAAC "A" sends an E-Mail message to the System Monitoring and Coordination Center (SMC) stating the problem and asks that the problem be resolved.

The SMC Resource Manager receives the request and retrieves a copy of the old and currently projected 30-day plan from DAAC "A". Upon review, he verifies that the delay is being caused by a change in the planned time of the data arrival from DAAC "B".

The SMC Resource Manager then retrieves a copy of the current and prior DAAC "B" 30-day plan. Upon review, he determines that a new algorithm integration and test activity has been scheduled for 8 hours at DAAC "B". He then reviews the plan for other ground activities and for the job priorities and types of production jobs scheduled at DAAC "B" for the day prior to the scheduled processing of the data required for DAAC "A". He notes there are no other ground activities that could potentially be modified and that, except for reprocessing requests, all production jobs have equal or higher priority than the job for DAAC "A".

The SMC Resource Manager then places a phone call to the DAAC "B" Production Scheduler. After discussing the problem, it is determined that the algorithm integration and test activity has a very high priority since the new algorithm is required for down- stream production runs and is being scheduled for implementation at the earliest possible date. In accordance with system policies and procedures, the SMC Resource Manager then asks the DAAC "B" Production Scheduler to resolve the problem by adjusting job priorities. After consulting with the DAAC "B" Manager, the Production Scheduler agrees to lower the priorities of the DAAC "B" reprocessing jobs that are scheduled a day prior to the job needed by DAAC "A" and to slightly raise the priority of the job for DAAC "A".

The DAAC "B" Production Scheduler generates a proposed new schedule using the altered priorities and notes that by lowering the priorities of the reprocessing requests, the job required by DAAC "A" can be completed 12 hours earlier. He saves the new projected plan and notifies the SMC Resource Manager by E-Mail. The SMC Resource Manager phones the DAAC "A" Production Scheduler and explains the status at DAAC "B" and informs him of the new plan. An agreement is reached that the new schedule is the best that can be achieved.

The SMC Resource Manager phones the DAAC "B" Production Scheduler and notifies him that the new plan is satisfactory and should be implemented. He then initiates the sending of E-Mail messages containing notification of the schedule changes to each affected DAAC. The DAAC "B" Production Scheduler then updates DAAC "B"'s production plan. The DAAC "A" Production Scheduler then regenerates the 30-day plan using the new schedule from DAAC "B".

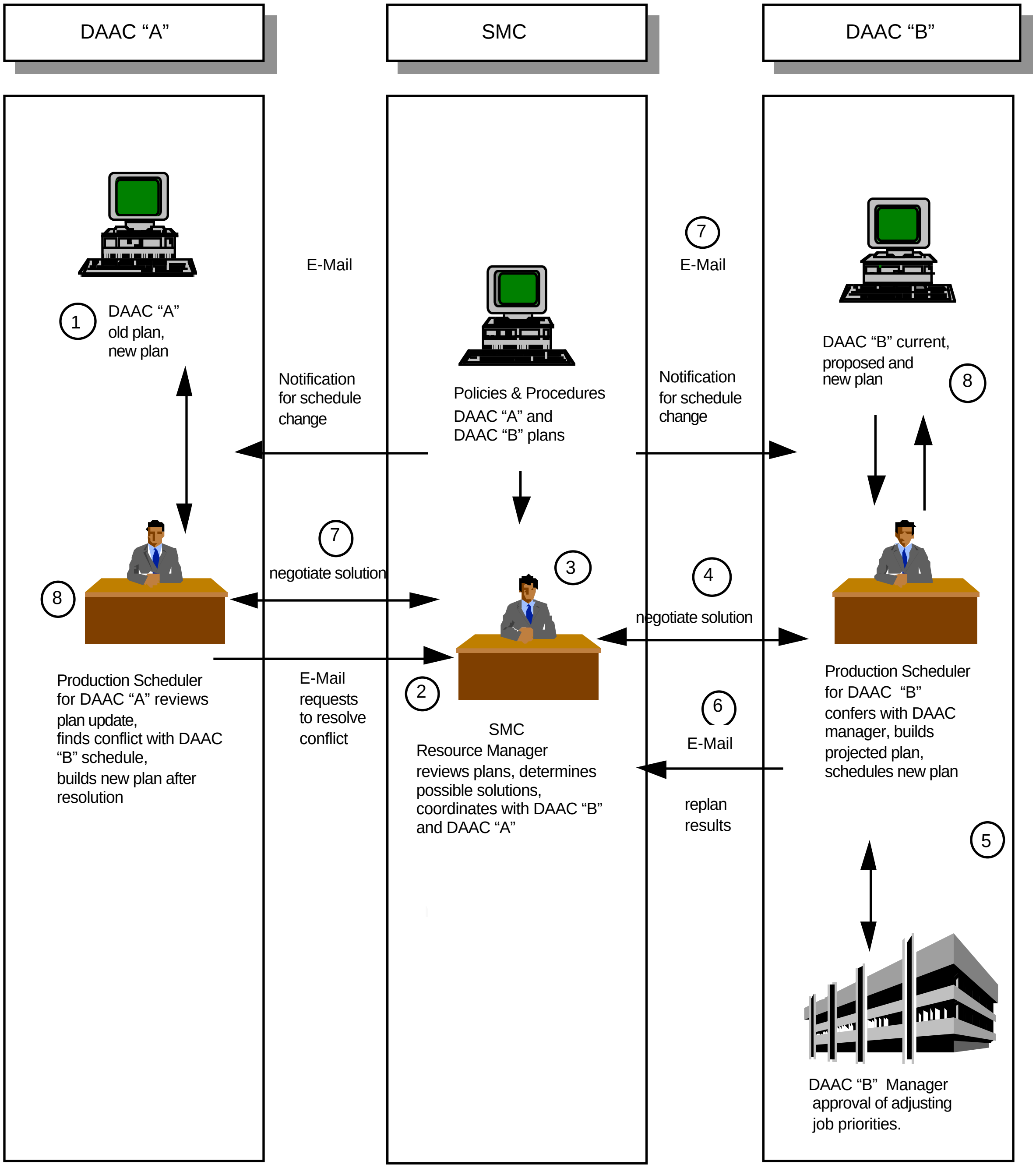


Figure 4.1.6.3-1. Schedule Adjudication Scenario

Table 4.1.6.3-1. Steps of the Scenario: Schedule Adjudication (1 of 2)

Scenario Assumptions: The production schedules are on a 30-day plan. The purpose of this scenario is to reach a compromise between the production schedule at DAAC "A" and the production schedule at DAAC "B". Upon discovering a delay in a high priority job scheduled 7 days from now, the Production Scheduler wants to avoid delays due to a change in the Data Availability Schedule from DAAC "B". Attempts to resolve the conflict directly between DAAC "A" and DAAC "B" were unsuccessful and, therefor, it must be adjudicated by the SMC.

Step	Operator/User	System	Purpose
1	DAAC "A" discovers a high priority job scheduled 7 days away that will have to be delayed a day due to a change in the Data Availability Schedule (DAS) from DAAC "B".	Projected 30-day plan is saved to server.	Notify Production Scheduler (PS) of potential changes.
2	Production Scheduler at DAAC "A" displays the revised 30-day plan and determines that the job priority warrants that the delay should be eliminated or reduced. He sends an E-Mail to the SMC stating the problem and asks that it be resolved.	Displays requested plan. Transmits E-Mail message from DAAC "A" PS.	Evaluate plan change. Alert the SMC of problem.
3	The SMC Resource Manager reviews current and prior DAAC "B" 30-day plan. Determines that a new algorithm integration and test activity has been scheduled. He reviews the plan for other ground activities, job priorities and types of production jobs scheduled at DAAC "B". He notes there are no other ground activities that could potentially be modified and that, except for reprocessing requests, all production jobs have equal or higher priority than the job for DAAC "A".	Displays DAAC "B" old and new plans.	Determine cause and possible solutions to schedule conflict.
4	The SMC Resource Manager phones the DAAC "B" Production Scheduler and discusses problem and possible solutions.		Find best solution to schedule conflict.
5	The DAAC "B" Production Scheduler confers with the DAAC "B" manager and agrees to lower the priorities of the DAAC "B" reprocessing jobs that are scheduled a day prior to the job needed by DAAC "A" and to slightly raise the priority of the job for DAAC "A".	Displays DAAC "B" 30-day plan. Adjusts priorities as specified by Production Scheduler. Displays new plan with adjusted priorities.	Produce proposed new 30-day plan.
6	The Production Scheduler notes that by lowering the priorities of the reprocessing requests, the job required by DAAC "A" can be completed 12 hours earlier. He saves the new projected plan and notifies the SMC Resource Manager by E-Mail.	Sends E-Mail message from Production Scheduler.	Evaluate the modified schedule.

Table 4.1.6.3-1. Steps of the Scenario: Schedule Adjudication (2 of 2)

Step	Operator/User	System	Purpose
7	The SMC Resource Manager phones the DAAC "B" Production Scheduler and notifies him that the new plan is satisfactory and should be implemented. He then initiates the sending of E-Mail messages containing notification of the schedule changes to each affected DAAC.	E-Mail is sent.	Verify change in schedule. Notify all parties of schedule change.
8	The DAAC "B" Production Scheduler then updates DAAC "B"'s production plan. The DAAC "A" Production Scheduler then regenerates the 30-day plan using the new schedule from DAAC "B".	New DAAC "B" 30-day plan is saved to server. New DAAC "A" 30-day plan is generated.	Regenerate 30-day plans.

4.1.6.4 Bad Data Scenario

See Figure 4.1.6.4-1 for a pictorial representation and Table 4.1.6.4-1 for a sequence of events for the Bad Data Scenario.

Only the process involving MSS is depicted in this scenario. For additional "Bad Data" scenarios refer to Science Data Ingest section 4.2.1, Science Data Archival section 4.2.2 and Production Processing section 4.2.5.

This scenario represents the MSS CSCI's interactions after a user has detected bad data and has written a trouble ticket. It is assumed that the "bad data" was produced within the last month. The DAAC Sustaining Engineer has determined that the data was corrupted by a hardware error.

The DAAC Sustaining Engineer sends an E-Mail message to the SMC Resource Manager identifying the bad data (and any other data products containing the bad data) by Universal Reference (UR) numbers. Using the URs, the SMC Resource Manager generates a query against the accounting database to produce a list of accounts receiving bad data, the bad data UR numbers per account, and the date and time it was delivered. He then retrieves and executes a script to send an E-Mail message to alert each recipient of the bad data. The E-Mail message specifies the date and time of each bad data item received and a notice that the account will receive a credit for each bad data item. The script run by the Resource Manager also sends the query results with an E-Mail message to SMC Accounting to credit each data recipient. SMC Accounting notifies the Billing Clerk to enter the credits into the accounting system.

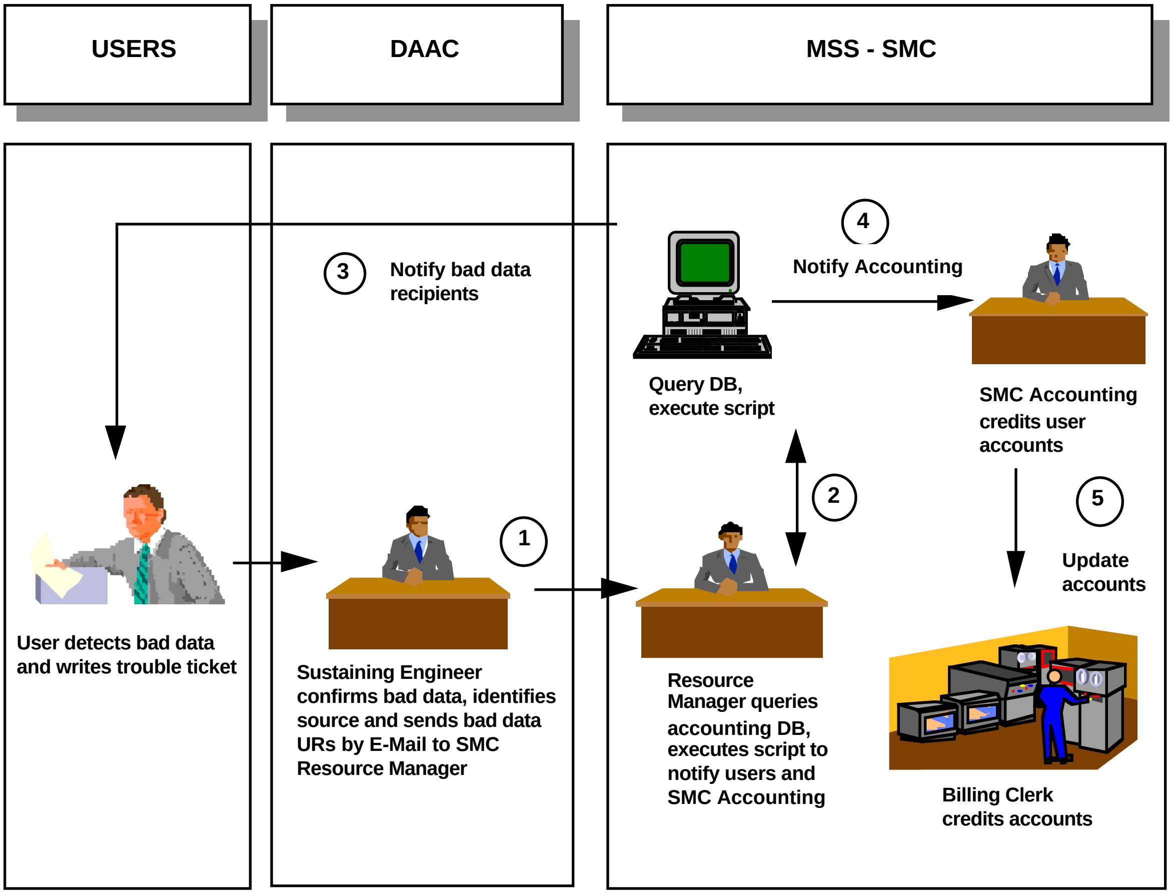

USERS
DAAC
MSS - SMC
3
Notify bad data recipients
4
Notify Accounting
Query DB, execute script
SMC Accounting credits user accounts
2
5
Update accounts
1
User detects bad data and writes trouble ticket
Sustaining Engineer confirms bad data, identifies source and sends bad data URs by E-Mail to SMC Resource Manager
Resource Manager queries accounting DB, executes script to notify users and SMC Accounting
Billing Clerk credits accounts

Figure 4.1.6.4-1. Bad Data Scenario

Table 4.1.6.4-1. Steps of the Scenario: Bad Data (1 of2)

Scenario Assumptions: A user has detected bad data. The user has notified ECS of the problem by sending an E-Mail message to trouble ticketing. The trouble ticket has been sent to the DAAC Sustaining Engineers who has determined that the data was corrupted by a hardware error.

Step	Operator/User	System	Purpose
1	The DAAC Sustaining Engineer sends an E-Mail message to the SMC Resource Manager identifying the bad data (and any other data products containing the bad data) by Universal Reference (UR) numbers.	Transmits E-Mail message.	To determine bad data recipients.
2	The Resource Manager generates a query against the accounting database to extract the ID of the accounts that received the bad data. The query results list several recipients.	Query is executed and the results returned.	Identify accounts receiving bad data and list bad data by account.

Table 4.1.6.4-1. Steps of the Scenario: Bad Data (2 of 2)

Step	Operator/User	System	Purpose
3	The Resource Manager then retrieves and executes a script to send an E-Mail message to alert each recipient of the bad data. The E-Mail message specifies the date and time of each bad data item received and a notice that the account will receive a credit for each bad data item.	Lists and executes script. Generates E-Mail messages.	Notify recipients that their data was bad.
4		Sends an E-Mail message to SMC Accounting to credit each data recipient.	Notify Accounting to correct accounts.
5	SMC Accounting notifies the Billing Clerk to enter the credits into the accounting system.	Credits are assigned.	Accounts are updated.